

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1, 3-38, and 40-49 are pending in the application, with claims 1, 15, 23, 31, 40, and 47 being independent. Claims 50-53 were previously canceled, and claims 2 and 39 are canceled herein without prejudice to or disclaimer of the subject matter recited therein. Claims 1, 3, 31, 33, 34, 38, 40, 41, 44, and 46 are amended herein. Support for the claim amendments and additions can be found in the original disclosure. No new matter has been added.

STATEMENT OF SUBSTANCE OF INTERVIEW

Initially, Applicant wishes to thank the Examiner for conducting an interview with Applicant's representative, Damon J. Kruger along with Elizabeth Zehr, on Wednesday September 3rd, 2008.

During the interview, Applicant's representative presented arguments distinguishing the claims from the cited references. In particular, Applicant's representative discussed claim 1 which was rejected under §103(a) and 35 U.S.C. § 112 second paragraph in the pending Office Action. Applicant's attorney and the Examiner were unable to reach an agreement as to amendments to claim 1; however, the Examiner indicated that more detail in claim 1, particularly relating to returning a pass or fail value based on the new set of rules would likely overcome the 35 U.S.C. § 112 second paragraph and move this case closer to allowance. Applicant thanks the Examiner for the above mentioned suggestions and has presented the claims accordingly.

The subject matter of the interview, and other remarks, are included below under their respective sections to assist the Examiner in more fully understanding the Applicant's position on the rejections under §103(a) and 35 U.S.C. § 112 second paragraph.

§ 112 SECOND PARAGRAPH REJECTIONS

Claims 1-4, 7-14, 31-34, 37-41, and 44-46, stand rejected under 35 U.S.C. § 112, as allegedly being incomplete for omitting essential steps, such omission amounting to a gap between the steps. In particular, the Office has repeated the following rejection with reference to Figure 3:

- 1) "Regarding claims 1-4, 7-14, the omitted steps are: steps 306-312 and 316,"
 - 2) "Regarding claims 31-34, 37-39, the omitted steps are: steps 306-310 and 316,"
- and
- 3) "Regarding claims 40-41, 44-46, the omitted steps are: steps 304-310 and 316."

This rejection is respectfully traversed. In particular, Applicant submits respectfully that claims 1, 31, and 40, as amended, include the alleged omitted steps. For discussion, Applicant focuses on claim 1 where the Office rejected claim 1 for omitting "steps" 306-312 and 316. As amended, claim 1 recites: "returning a fail value when each of the plurality of security engines has determined that it is not ready to begin using the new security policy" (Step 310); "returning a pass value when each of the plurality of security engines has determined that it is ready to begin using the new security policy" (Step 308); and "continue operating each of the plurality of security engines according to

the previous rules when at least one of the plurality of security engines has determined that it is not ready to begin using the new security policy” (Steps 306, 312 and 316).

Claims 2-4, and 7-14 depend from independent claim 1 and are thus in compliance with 35 U.S.C. §112, second paragraph by virtue of this dependency. Similarly, claims 32-34 and 37-39 depend from claim 31; and claims 41 and 44-46 depend from claim 40 and are thus similarly in compliance with 35 U.S.C. §112, second paragraph by virtue of this dependency.

Therefore, Applicants respectfully request reconsideration and withdrawal of the rejection to claims 1-4, 7-14, 31-34, 37-41, and 44-46.

§ 103 REJECTIONS

Claims 1-2 and 7-13 stand rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent Publication No. 2005/0044418 (“Miliefsky”) in view of U.S. Patent Publication No. 2004/0003266 (“Moshir”).

Claims 3-4 and 14 stand rejected under 35 U.S.C. § 103(a) as being obvious over Miliefsky in view of Moshir and further in view of “An Introduction to Database System” (“Date”).

Claims 31-34, 37-41, and 44-46 stand rejected under 35 U.S.C. § 103(a) as being obvious over Moshir in view of Date.

Applicant respectfully traverses the aforementioned rejections, and further requests that the rejections be reconsidered and withdrawn for at least the reasons that follow.

Independent claim 1, as presently presented, is directed to “A method, implemented in a computing device”, and recites:

A method, implemented in a computing device, the method comprising:

accessing a new security policy to be implemented by a plurality of security engines of the computing device and to be implemented by the plurality of security engines in place of a current security policy;

each of the plurality of security engines processing at least a portion of the new security policy to establish new rules for operation of the security engine while the security engine continues to operate according to previous rules;

returning a fail value when each of the plurality of security engines has determined that it is not ready to begin using the new security policy;

returning a pass value when each of the plurality of security engines has determined that it is ready to begin using the new security policy;

receiving an indication to ignore the new set of rules and continue operating each of the plurality of security engines according to the previous rules when at least one of the plurality of security engines has determined that it is not ready to begin using the new security policy; and

switching, after receiving an indication that each of the plurality of security engines has determined it is ready to begin using the new security policy, each of the plurality of security engines to the new rules substantially concurrently. (Emphasis added).

Miliefsky is directed to providing “proactive network security systems that protect against hackers and may automatically find, report, and communicate with countermeasures and remove the common vulnerabilities and exposures (CVEs) that they exploit.” (Summary). However, Miliefsky fails to disclose or suggest “receiving an indication to ignore the new set of rules and continue operating each of the plurality of security engines according to the previous rules when at least one of the plurality of

security engines has determined that it is not ready to begin using the new security policy” as presently recited in independent claim 1.

Moshir generally pertains to discovering software updates, discovering if a given computer can use the software update, and then updating the computers with software as needed automatically across a network without storing the updates on an intermediate machine within the network. (Summary). In addition, Moshir pertains to detecting failures, stopping a rollout, and removing software from computers that were already updated. (Id.).

Moshir fails to remedy the deficiencies in Miliefsky noted above with respect to claim 1. Specifically, Moshir teaches detecting for failures after the machines have begun to operate under the updated security policy rather than “receiving an indication to ignore the new set of rules and continue operating each of the plurality of security engines according to the previous rules when at least one of the plurality of security engines has determined that it is not ready to begin using the new security policy”.

Moshir recites:

If there are multiple target computers 500, failure may be detected by the monitor *after the software has been installed* on one or more machines. In this case, the software update can be removed 322 from not only the target computer 500 where the failure was spotted, but it can also be removed 326 from all of the other target computers 500 *where the software was previously installed* 326. (Paragraph [0077], Emphasis added).

As recognized by the Office, “the new/updated security policy is not in effect until the installing step is completed (i.e., until it is installed).” (Office Action page 3, lines 1-2).

Thus, in Moshir, if a failure is detected, it is not removed “from all of the other target

computers 500 where the software was previously installed” until “after the software has been installed on one or more machines” (i.e. until after the new/updated security policy has taken effect). This is not the equivalent of “*receiving an indication to ignore the new set of rules*” as recited in claim 1.

Claim 1 is supported by the specification on at least page 18, line 25 through page 19, line 8. Accordingly, independent claim 1 is believed allowable.

Dependent claims 7 and 7-13 depend from independent claim 1 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Dependent claims 3, 4, and 14 depend from independent claim 1 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Independent claim 31, as presently presented, is directed to “One or more computer readable storage media having one or more instructions”, and recites:

One or more computer readable storage media storing one or more instructions that, when executed by one or more processors, causes the one or more processors to:

receive information of a new security policy to be used;

generate a new set of rules having associated data based on the new security policy;

returning a fail value when it is determined that the new set of rules are not ready for use;

returning a pass value it is determined that the new set of rules are ready for use;

continue to use a previous set of rules and associated data when it is determined that the new set of rules are not ready for use;
and

using, upon receiving an indication that the new set of rules are ready for use , the new set of rules and associated data. (Emphasis added).

Moshir either singly or in view of Date fails to disclose or suggest “continue to use a previous set of rules and associated data when it is determined that the new set of rules are not ready for use” as presently recited in independent claim 31.

Applicant incorporates similar reasoning as presented above in response to the rejection of claim 1. Specifically, Moshir teaches detecting for failures after the machines have begun to operate under the updated security policy which is not the equivalent of “continue to use a previous set of rules and associated data when it is determined that the new set of rules are not ready for use.”

Furthermore, Date fails to remedy the deficiencies of Moshir. Rather, the Office relies on Date for allegedly teaching “a two-phase commit protocol used in an update operation involving multiple participants whereby each participant receives a system-wise commit command if all the participants have successfully processed the update (page 463).” (Office Action page 7, lines 9-12). Accordingly independent claim 31 is believed allowable.

Dependent claims 32-34 and 37-38 depend from independent claim 31 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Independent claim 40, as presently presented, is directed to “A Multiple System Operation system”, and recites:

A method, implemented in a security engine of a computing device, the method comprising:
receiving a new set of rules to be enforced;
returning a fail value when each of the plurality of security engines has determined that it is not ready to begin using the new security policy;
returning a pass value when each of the plurality of security engines has determined that it is ready to begin using the new security policy;
receiving an indication to ignore the new set of rules and continue using a previous set of rules when it is determined that the new set of rules are not ready for use ; and
enforcing, in response to receipt of an indication that it is determined that the new set of rules are ready for use, the new set of rules. (Emphasis added).

Moshir either singly or in view of the cited art fails to disclose or suggest "receiving an indication to ignore the new set of rules and continue using a previous set of rules when it is determined that the new set of rules are not ready for use" as presently recited in independent claim 40.

Applicant incorporates similar reasoning as presented above in response to the rejection of claim 1. Specifically, Moshir teaches detecting for failures after the machines have begun to operate under the updated security policy which is not the equivalent of "receiving an indication to ignore the new set of rules and continue using a previous set of rules when it is determined that the new set of rules are not ready for use."

Accordingly independent claim 40 is believed allowable.

Dependent claims 41, and 44-46 depend from independent claim 40 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

CONCLUSION

For at least the foregoing reasons, claims 1, 3-4, 7-14, 31-34, 37-38, 40, 41, and 44-46 are in condition for allowance. Applicant respectfully requests reconsideration and withdrawal of the rejections and an early notice of allowance.

The arguments and amendments presented herein were necessitated by the most recent Office Action, and could not have been presented previously because Applicant earnestly believed that the claims were in condition for allowance at the time of filing the previous response.

If any issue remains unresolved that would prevent allowance of this case, Applicant requests that the Examiner contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Lee & Hayes, PLLC

Dated: September 29, 2008

By: David S. Lee

David S. Lee
Reg. No. 38222
206-315-7912